VIIS Internal User Add-On Forms

The following information is for VIIS administrators who wish to give additional individuals within their organization access to VIIS. They are responsible for distributing and maintaining the paperwork as well as determining the proper security role for new users and activating them in the applications. (Click here to see more detail)

STEP 1: Have each individual complete the following three forms.

- VIIS User Registration Form
- VIIS Security Policy & User Confidentiality Agreement
- VDH Information Systems Security Access Agreement

STEP 2: The assigned administrator is to maintain these forms.

*IMPORTANT NOTE: These forms DO NOT need to be mailed to VDH.

Virginia Immunization Information System (VIIS) User Registration Form*

Administrators must fill out entire form
Users fill ONLY fill the sections highlighted in BLUE.

1. User Name:

_____

Printed Name, Title Signature Date

2. License number: _____

3. Phone: (_____)_____

4. Fax: (_____)_____

5. Alternate Phone: (_____)_____

6. Email: _____

7. Organization/Site Name: _____

8. VIIS Organization Code/Site Code _____
(If Known)

9. Address:

_____

_____

10. Approving Practitioner:

_____

Printed Name, Title Signature Date

13. Alternate Phone: (_____)_____

14. Email: _____

VIIS Security Policy & User Confidentiality Agreement

VIIS Information:

The Code of Virginia, § 32.1-46.01 authorizes the Virginia Immunization Information System (VIIS), a statewide immunization information system that manages electronic immunization records. This policy states behaviors required of VIIS users, Virginia Department of Health (VDH), and Division of Immunization (DOI) to protect the confidentiality, privacy and accuracy of client information.

1. VIIS is consistent with the Department of Health and Human Services and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
2. Authorized users of VIIS will include:
   a. Health care provider or health plans
   b. Schools or other organizations that provide health care services
   c. Individuals or organizations as required by law or in the management of a public health crisis
   d. Other immunization registries
3. The review of this policy must involve the participation of representatives from the private and public health care sectors.

VDH/DOI Host Site Security:

1. The system will force users to change their password every 30 days.
2. The VIIS system will time-out after 45 minutes.
3. No information from VIIS will be made available to law enforcement, the Immigration and Naturalization Service, or any other party.
4. The VIIS system will maintain an audit trail for all information accessed.
5. VDH/ EDS will conduct a self-assessment of the potential risks and areas of vulnerability regarding VIIS and will develop, implement, and maintain appropriate security measures on an ongoing basis.
6. The release of immunization information shall be for statistical purposes or for studies that do not identify individuals.

Provider/ User Security:

1. Access to VIIS information is authorized under the condition that it is required to perform my job function
2. All VIIS users will be required to sign a Confidentiality/ Security Agreement with VDH
3. Each user must renew the user confidentiality/security agreement every two years.
4. Each user is responsible for maintaining confidentiality.
5. The provider will specify that the user has the obligation to act on any request by an individual to opt out of VIIS. If the patient elects to opt out, the provider should promptly mark the record in VIIS as “Do Not Share”, so that only that provider may view the client’s immunization records
6. The user will make reasonable effort to ensure the accuracy of all immunization and demographic information entered or edited
7. Virus protection is recommended for each client site.
8. User desktops/laptops must have physical security and password screen savers when not being used by authorized individuals and will terminate the VIIS application prior to leaving the VIIS workstation
9. An ID and Password are required to access VIIS.
10. Users will not share or disclose their ID or password to anyone.
11. The VIIS Administrator will maintain completed user registration forms in a secure location
12. All data from VIIS will be encrypted before transfer.
13. VIIS records will be treated with the same vigilance, confidentiality, and privacy as any other patient medical record.
14. Patient immunization records will not be copied except for authorized use
15. VIIS information in a paper copy will not be left where it would be visible for unauthorized personnel and must be shredded before disposal

16. Unauthorized disclosure of information from confidential records may be punishable, upon conviction, by a fine and/or imprisonment or both, and/or civil penalties as prescribed by law as well as sanctions and/or disciplinary action.
17. If VIIS data is to be faxed, the sender must verify the fax number and receipt of data.
18. Any activity that would jeopardize the proper function/security of VIIS will not be conducted. Misuse of VIIS may result in legal action against me personally, and against the organization for which I am an agent

Provider Responsibility:

1. A copy of this agreement has been provided to me
2. The VIIS Administrator at the user site will terminate access for an authorized user who no longer requires access.
3. Users will make every effort to protect VIIS screens from unauthorized view.
4. Should a material breach of personal privacy/confidentiality occur, the offending party must immediately notify the client and VDH/ DOI designee. Violators of this policy will be restricted from VIIS by the System Administrator at the offender's site.
5. The VIIS Administrator will be notified immediately if unauthorized entry into the system is suspected.

Approved by:

To be signed by one representative that has the delegated authority to act on behalf of the User organization and one representative that has the delegated authority to act on behalf of VDH/DOI.

_____
User Company/Organization Name (Print)

_____	_____
Name of Authorized Agent (Print)	Name of Authorized Agent (Print)
_____	_____
Signature of Authorized Agent	Signature of Authorized Agent
_____	_____
Title	Title
_____	_____
Date	Date

Reviewed on 11-02-2007

Commonwealth of Virginia
Department of Health
Information Systems Security Access Agreement

As a user of the Department of Health (VDH) information systems, I understand and agree to abide by VDH Security Policy and the following terms which govern my access to and use of the information and computer services of VDH.

Access has been granted to me by VDH as a necessary privilege in order to perform my authorized job functions for VDH. Passwords and logon IDs should not be shared. I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as Logon IDs, passwords, terminal IDs or file protection) for any purposes other than those required to perform my authorized employment functions. I agree to change passwords immediately if they are compromised. I will not incorporate passwords into any sign on software.

If, due to my authorized job functions, I require access to information on VDH information systems which are not owned by my division, I must obtain authorized access to that information from the information owner and present access documentation to Data Administration (Office of Information Management).

I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so, and I will not use access mechanisms which have not been expressly assigned to me. I will not use VDH systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates or issues.

Having read the VDH Security Awareness Web site and corresponding sections on Personal Computer (PC) Use, Computer Access Security, and Data Security in the VDH Information Technology Resources Policy and Procedures Manual, I certify that I have received Computer Security Awareness training and understand my security responsibilities as a user of the Department of Health (VDH) information systems.

I agree to abide by all applicable Federal, Commonwealth of Virginia, and VDH agency policies, procedures and standards which relate to the security of VDH information systems and the data contained therein.

If I observe incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the information Security Officer and management of VDH.

I give consent to the monitoring of my activities on VDH information systems, and other systems accessed through VDH systems.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action according to the State Employee Rules of Conduct, including but not limited to the termination of my access privileges.

_____	_____
Employee/Consultant Name (Print)	Date of Signature
_____	_____
Employee/Consultant Signature	Division Name